UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,301	08/16/2001	Steven Black	AUS920010242US1	3154

35525 7590 04/21/2005

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 04/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,301	BLACK ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 February 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 21 have been presented for examination.

Response to Arguments

2. Applicant's arguments filed on 2/7/2005 have been fully considered but are not persuasive.

3. As per claim 1, 8 and 15, Applicant argues: "Molini does not teach classifying events as groups by aggregating events with at least one attribute within the event set as an identical value".

4. Examiner notes, first of all, the event is interpreted as an undesired behavior pattern observed from a series of alarm messages with the following event attributes: source of attack, destination of attack and type of event or intrusion (or attack) (Molini: see for example, Column 5 Line 4 – 7). Secondly, Molini teaches classified the event groups with the appropriate severity level / priority level based on the determination whether the minimum threshold has been exceeded or not after aggregating those events with at lease one attribute with an identical value within the event set (Molini: see for example, Column 7 Line 5 – 6, Column 7 Line 35 – 37, Column 7 Line 50 – 55, Column 7 Line 60 – 61 and Column 5 Line 4 – 7). Examiner interprets "the attribute with an identical value within the event set" as, for example, unauthorized access type and particular computers (i.e. the same network address) to meet the claim language (Molini: see for example, Column 7 Line 60 – 61).

5. Therefore, Molini does teach classifying events as groups by aggregating events with at least one attribute within the event set as an identical value.

6. As per claim 2, 9 and 16, Applicant argues: "Molini does not teach that severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups" (Page 9, 5th Paragraph). See the same rationale applied herein as above for claim 1.

7. As per claim 4, 11 and 18, Applicant argues: "Molini does not teach that calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group" (Page 11, 2nd Paragraph).

8. Examiner notes Molini teaches calculating the threshold by assigning a fixed number to the event group (Molini: see for example, Column 7 Line 56 – 57 and Column 7 Line 60 – 61: The threshold must be a fixed number so that whether greater than or equal to 10% of the threshold has been exceeded can be determined). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1 – 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Molini (Patent Number: US 6353385 B1).

As per claim 1, 8 and 15, Molini teaches a method in a data processing system for reporting security situations, comprising the steps of:

logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute (Molini, see example, Column 5 Line 4 – 7, Column 7 Line 5 – 6 and Column 9 Line 24 – 29: an undesired behavior pattern observed from a series of alarm messages with the following event attributes: source of attack, destination of attack and type of event or intrusion (or attack);

classifying events as groups by aggregating events with at least one attribute within the event set as an identical value (Molini, see example, Column 7 Line 5 – 6, Column 7 Line 35 – 37, Column 7 Line 50 – 55, Column 7 Line 60 – 61 and Column 5 Line 4 – 7: Molini teaches classified the event groups with the appropriate severity level

/ priority level based on the determination whether the minimum threshold has been exceeded or not after aggregating those events with at lease one attribute with an identical value within the event set. Examiner interprets "the attribute with an identical value within the event set" as, for example, unauthorized access type and particular computers (i.e. the same network address) to meet the claim language (Molini: see for example, Column 7 Line 60 – 61) and (Molini, see example, Column 8 Line 25 – 37, Column 7 Line 19 – 20, Column 6 Line 49 – 51 and Column 9 Line 30 – 35); and

calculating severity levels for the groups (Molini, see example, Column 7 Line 54 and Column 7 Line 33: The severity level is set by a formula depending upon whether greater than or equal to 10% of the threshold has been exceeded or not. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value (Molini, see example, Column 7 Line 50 – 55 and Figure 1 Element 30 and 35).

As per claim 2, 9 and 16, Molini teaches the claimed invention as described above (see claim 1, 8 and 15 respectively). Molini further teaches the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of

the event sets within each of the groups. See the same rationale applied herein as above for claim 1 (Molini: see for example, Column 7 Line 5 – 6, Column 7 Line 35 – 37, Column 7 Line 50 – 55, Column 7 Line 60 – 61, Column 5 Line 4 – 7) & (Molini, see example, Column 7 Line 27 – 40 and Column 8 Line 48 – 55).

As per claim 3, 10 and 17, Molini teaches the claimed invention as described above (see claim 1, 8 and 15 respectively). Molini further teaches the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation (Molini, see example, Column 1 Line 60 – 62 and Column 3 Line 36 – 38).

As per claim 4, 11 and 18, Molini teaches the claimed invention as described above (see claim 1, 8 and 15 respectively). Molini further teaches calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group (Molini, see example, Column 7 Line 56 – 57 and Column 7 Line 60 – 61: The threshold must be a fixed number so that whether greater than or equal to 10% of the threshold has been exceeded can be determined) and (Molini, see example, Column 7 Line 50 – 63 and Column 8 Line 48 – 55).

As per claim 5, 12 and 19, Molini teaches the claimed invention as described above (see claim 1, 8 and 15 respectively). Molini further teaches the target attribute represents one of a computer and a collection of computers (Molini, see example, Column 1 Line 29 – 35).

As per claim 6, 13 and 20, Molini teaches the claimed invention as described above (see claim 1, 8 and 15 respectively). Molini further teaches the source attribute represents one of a computer and a collection of computers (Molini, see example, Column 1 Line 29 – 35).

As per claim 7, 14 and 21, Molini teaches the claimed invention as described above (see claim 1, 8 and 15 respectively). Molini further teaches aggregating a subset of the groups into a combined group (Molini, see example, Column 9 Line 30 – 32).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Burrows (U.S. Patent Publication Number: 2002/0073338) discloses "Method and System fir Impacting the Impact of Undesirable Behavior of Computers on a Shared Data Network" – (for example, Paragraph [0046]).

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100